PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-012688
(43)Date of publication of application : 13.01.2005

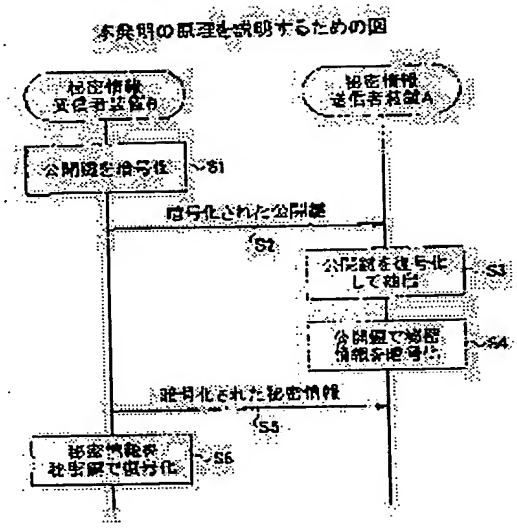
(51)Int.Cl. H04L 9/08
G06T 1/00
G09C 5/00
H04N 1/387

(21)Application number : 2003-176960
(22)Date of filing : 20.06.2003

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : KATAYAMA ATSUSHI
NAKAMURA TAKAO
SONEHARA NOBORU

(54) SECRET CORRESPONDENCE PROCEDURE, SYSTEM, AND TERMINAL EQUIPMENT

(57)Abstract:
PROBLEM TO BE SOLVED: To keep content secret even if an arbitrary third person acquires transmitted information by simplifying receiving of an electronic watermark key when secretly communicating the information.
SOLUTION: A disclosing key is coded with a device at the side of a secrete information receiving person to be delivered to a secret information transmitting person. The electronic water mark key used for hiding secret information is generated with the device at the side of secret information transmitting person every time, and generated random number is coded with a disclosing code system to be attached or hidden to an image to be transmitted to the device at the side of a secret information receiving person.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-12688
(P2005-12688A)
(43)公開日　平成17年1月13日(2005.1.13)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/08	H04L	9/00	601C	5B057
G06T	1/00	G06T	1/00	500B	5C076
G09C	5/00	G09C	5/00		5J104
H04N	1/387	H04N	1/387		
		H04L	9/00	601E	

審査請求 未請求　請求項の数 19　OL　（全 19 頁）

(21)出願番号　特願2003-176960(P2003-176960)
(22)出願日　平成15年6月20日(2003.6.20)

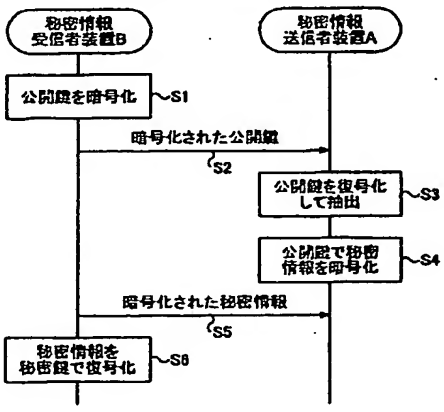
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　片山　淳
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　中村　高雄
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　曽根原　登
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】秘匿通信方法及びシステム及び端末装置

(57)【要約】
【課題】情報を秘匿して通信する際に、電子透かし鍵の授受を簡易化し、送信された情報を任意の第三者が取得したとしてもその内容を知ることができないようにする。
【解決手段】本発明は、秘密情報受信者側の装置で公開鍵を暗号化して、秘密情報送信者に渡し、秘密情報送信者側の装置で、秘密情報埋め込みに用いる電子透かしの鍵を通信の都度生成し、生成した乱数を公開鍵暗号方式で暗号化して、画像に添付する、又は、埋め込んで、秘密情報受信者側の装置に送信する。
【選択図】　図１

本発明の原理を説明するための図



【特許請求の範囲】
【請求項１】
秘密情報送信者Ａの秘密情報を秘密情報送信者装置（以下送信装置と記す）Ａから秘密情報受信者Ｂの秘密情報受信者装置（以下受信装置と記す）Ｂに伝達する秘匿通信方法において、
前記受信装置Ｂにおいて、前記受信者Ｂの公開鍵を第三者に対して復号方法が公知な暗号化方法により暗号化する、鍵暗号化ステップと、
前記受信装置Ｂにおいて、暗号化した公開鍵を前記送信装置Ａに送る公開鍵送信ステップと、
前記送信装置Ａにおいて、前記受信装置Ｂから受信した前記公開鍵を復号化して公開鍵を取り出す公開鍵抽出ステップと、
前記送信装置Ａにおいて、取り出した前記公開鍵により前記送信者Ａの秘密情報を暗号化する秘密情報暗号化ステップと、
前記送信装置Ａにおいて、暗号化された秘密情報を前記受信装置Ｂに送信する秘密情報送信ステップと、
前記受信装置Ｂにおいて、前記暗号化された秘密情報を受信して、該受信装置Ｂのみが有する秘密鍵を用いて復号化して秘密情報を得る秘密情報復号化ステップと、
からなることを特徴とする秘匿通信方法。
【請求項２】
前記鍵暗号化ステップにおいて、
前記復号方法が公知な暗号化方式として、読み出し方法が公知である電子透かし情報埋め込み技術を用いる請求項１記載の秘匿通信方法。
【請求項３】
前記公開鍵送信ステップにおいて、
前記受信装置Ｂが、前記電子透かしにより前記公開鍵を埋め込んだ画像を前記送信装置Ａに提示し、
前記送信装置Ａにおいて、
提示された前記画像をカメラで撮影するステップを含む請求項２記載の秘匿通信方法。
【請求項４】
前記公開鍵送信ステップにおいて、
前記受信装置Ｂが、前記電子透かしにより前記公開鍵を埋め込んだ画像を、電子メールにより前記送信装置Ａに送る請求項２記載の秘匿通信方法。
【請求項５】
前記公開鍵送信ステップにおいて、
前記受信装置Ｂが、前記電子透かしにより前記公開鍵を埋め込んだ画像を、サーバにアップロードするステップを含み、
前記公開鍵抽出ステップにおいて、前記送信装置Ａが、前記サーバにアップロードされた画像をダウンロードするステップを含む請求項２記載の秘匿通信方法。
【請求項６】
前記公開鍵送信ステップにおいて、
前記受信装置Ｂが、前記電子透かしにより前記公開鍵を埋め込んだ画像を、サーバにアップロードするステップを含み、
前記公開鍵抽出ステップにおいて、前記送信装置Ａが、前記サーバにアップロードされた画像をインターネットブラウザにより閲覧するステップを含む請求項２記載の秘匿通信方法。
【請求項７】
前記秘密情報暗号化ステップにおいて、
前記送信装置Ａが、乱数を電子透かし埋め込み鍵にして、前記秘密情報を任意の画像に埋め込み、該乱数を前記公開鍵により暗号化して電子透かし埋め込み済み画像に添付するステップを含む請求項１乃至６記載の秘匿通信方法。

【請求項８】
前記秘密情報暗号化ステップにおいて、
前記送信装置Ａが、乱数を電子透かし埋め込み鍵にして、前記秘密情報を任意の画像に埋め込み、該乱数を前記公開鍵により、暗号化したものを読み出し方法が公知の電子透かし方法を用いて、電子透かし埋め込み済み画像に２重に埋め込むステップを含む請求項１乃至６記載の秘匿通信方法。
【請求項９】
秘密情報送信者Ａの秘密情報を秘密情報送信者装置（以下、送信装置と記す）Ａから秘密情報受信者Ｂの秘密情報受信者装置（以下、受信装置と記す）Ｂに伝達する秘匿通信システムであって、
前記受信装置Ｂは、
前記受信者Ｂの公開鍵を第三者に対して復号方法が公知な暗号化方法により暗号化する、鍵暗号化手段と、
前記鍵暗号化手段で暗号化した公開鍵を前記送信装置Ａに送る公開鍵送信手段と、
前記送信装置Ａから暗号化された秘密情報を受信して、当該受信装置Ｂのみが有する秘密鍵を用いて復号化して秘密情報を得る秘密情報復号化手段と、
を有し、
前記送信装置Ａは、
前記受信装置Ｂから受信した前記公開鍵を復号化して公開鍵を取り出す公開鍵抽出手段と、
前記公開鍵抽出手段で取り出した前記公開鍵により前記送信者Ａの秘密情報を暗号化する秘密情報暗号化手段と、
前記秘密情報暗号化手段において、暗号化された秘密情報を前記受信装置Ｂに送信する秘密情報送信手段と、
を有することを特徴とする秘匿通信システム。
【請求項１０】
前記鍵暗号化手段は、
前記復号方法が公知な暗号化方式として、読み出し方法が公知である電子透かし情報埋め込みを用いる請求項９記載の秘匿通信システム。
【請求項１１】
前記受信装置の前記公開鍵送信手段は、
前記電子透かしにより前記公開鍵を埋め込んだ画像を前記送信装置Ａに提示する手段を含み、
前記送信装置Ａの前記公開鍵抽出手段は、
前記電子透かしにより前記公開鍵が埋め込まれた画像をカメラで撮影する手段を含む請求項１０記載の秘匿通信システム。
【請求項１２】
前記受信装置の前記公開鍵送信手段は、
前記電子透かしにより前記公開鍵を埋め込んだ画像を、電子メールにより前記送信装置Ａに送る手段を含む請求項１０記載の秘匿通信システム。
【請求項１３】
前記受信装置Ｂの前記公開鍵送信手段は、
前記電子透かしにより前記公開鍵を埋め込んだ画像を、サーバにアップロードする手段を含み、
前記送信装置Ａの前記公開鍵抽出手段は、
前記サーバにアップロードされた画像をダウンロードする手段を含む請求項１０記載の秘匿通信システム。
【請求項１４】
前記受信装置Ｂの前記公開鍵送信手段は、
前記電子透かしにより前記公開鍵を埋め込んだ画像を、サーバにアップロードする手段含

み、
前記送信装置Ａの前記公開鍵抽出手段は、
前記サーバにアップロードされた画像をインターネットブラウザにより閲覧する手段を含む請求項１０記載の秘匿通信システム。
【請求項１５】
前記送信装置Ａの前記秘密情報暗号化手段は、
乱数を電子透かし埋め込み鍵にして、前記秘密情報を任意の画像に埋め込み、該乱数を前記公開鍵により暗号化して電子透かし埋め込み済み画像に添付する手段を含み、
前記受信装置Ｂの秘密情報復号化手段は、
前記電子透かし埋め込み済み画像に添付された暗号化された前記乱数を自分の秘密鍵で復号し、元の乱数を取得し、該乱数を電子透かし読み出し鍵として、該画像から秘密情報を取得する手段を含む請求項９乃至１４記載の秘匿通信システム。
【請求項１６】
前記送信装置Ａの前記秘密情報暗号化手段は、
乱数を電子透かし埋め込み鍵にして、前記秘密情報を任意の画像に埋め込み、該乱数を前記公開鍵により、暗号化したものを読み出し方法が公知の電子透かし方法を用いて、電子透かし埋め込み済み画像に２重に埋め込む手段を含み、
前記受信装置Ｂの秘密情報復号化手段は、
前記電子透かし埋め込み画像から公知の電子透かし読み出し方法により暗号化された乱数を取得し、該乱数を自分の秘密鍵で復号し、復号された乱数を電子透かし読み出し鍵として、該電子透かし埋め込み画像から秘密情報を取得する手段を含む請求項９乃至１４記載の秘匿通信システム。
【請求項１７】
秘密情報の送受信を行う端末装置であって、
公開鍵を第三者に対して復号方法が公知な暗号化方式として、読み出し方法が公知である電子透かし情報埋込技術を用いて暗号化し、画像に埋め込む、鍵暗号化手段と、
前記鍵暗号化手段で暗号化した公開鍵が埋め込まれた画像を、前記秘密情報を送信する送信装置に送る公開鍵送信手段と、
前記送信装置から暗号化された秘密情報を受信して、自装置のみが有する秘密鍵を用いて復号化して秘密情報を得る秘密情報復号化手段と、
前記秘密情報を受信する受信装置から受信した、画像に埋め込まれた公開鍵を抽出して、復号化する公開鍵抽出手段と、
前記公開鍵抽出手段で取り出した前記公開鍵により前記送信者側の秘密情報を暗号化する秘密情報暗号化手段と、
前記秘密情報暗号化手段において、暗号化された秘密情報を前記受信装置に送信する秘密情報送信手段と、
を有することを特徴とする端末装置。
【請求項１８】
前記秘密情報暗号化手段は、
乱数を生成し、該乱数を電子透かし埋込鍵として、前記秘密情報を任意の画像に埋め込み、該乱数を前記公開鍵により暗号化して、電子透かし埋め込み済み画像に添付する手段を含み、
前記秘密情報復号化手段は、
暗号化された前記乱数を自らの秘密鍵を用いて復号化し、復号化された乱数を受信した画像に埋め込まれている電子透かしの読み出し鍵として、埋め込み済み画像から秘密情報を取得する手段を含む請求項１７記載の端末装置。
【請求項１９】
前記秘密情報暗号化手段は、
乱数を生成し、該乱数を電子透かし埋め込み鍵にして、前記秘密情報を任意の画像に埋め込み、該乱数を前記公開鍵により、暗号化したものを読み出し方法が公知の電子透かし方

法を用いて、電子透かし埋め込み済み画像に２重に埋め込む手段を含み、
前記秘密情報復号化手段は、
前記公知の電子透かし読み出し方法を用いて、受信した画像に埋め込まれている暗号化乱数を取得し、該暗号化乱数を自らの秘密鍵で復号することにより乱数を取得し、該乱数を電子透かし読み出し鍵として、埋め込み済み画像から秘密情報を取得する手段を含む請求項１７記載の端末装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、秘匿通信方法及びシステム及び端末装置に係り、特に、送信者の秘密情報を受信者に伝達する情報伝達過程における秘匿通信方法及びシステム及び端末装置に関する。

【０００２】

【従来の技術】

情報を秘匿して通信する秘密通信技術では、情報を伝達するメディアとして、通信自体が自然であるためと、情報を埋め込んだことが分かりにくいため、画像が多用される。画像に情報を埋め込む技術には電子透かしが利用される（例えば、非特許文献１参照）。

【０００３】

【非特許文献１】

『インフォメーションハイディングの技術調査報告書』平成１０年２月、
情報処理進行事業協会、
「ｈｔｔｐ：／／ｗｗｗ．ｉｐａ．ｇｏ．ｊｐ／ｓｅｃｕｒｉｔｙ／ｆｙ１０／ｃｏｎｔｅｎｔｓ／ｃｒｙｐｔｏ／ｒｅｐｏｒｔ／Ｉｎｆｏｒｍａｔｉｏｎ－Ｈｉｄｉｎｇ．ｈｔｍ」

【０００４】

【発明が解決しようとする課題】

しかしながら、上記の電子透かし技術では情報埋め込みに用いる鍵と読み出しに用いる鍵が同一のため、秘匿通信の送信者と受信者で電子透かし鍵情報を予め共有しなければならず、電子透かし鍵の授受の簡便さと、鍵の守秘管理の厳密さが相反するという問題がある。

【０００５】

また、情報の通信相手をも秘匿したい場合においても、電子透かし鍵を渡す行為から通信相手が第三者に知られてしまうという問題がある。

【０００６】

本発明は、上記の点に鑑みなされたもので、電子透かし鍵の授受を簡易化し、かつ、送信された情報を任意の第三者が取得したとしてもその内容を知ることができない秘匿通信方法及びシステム及び端末装置を提供することを目的とする。

【０００７】

【課題を解決するための手段】

図１は、本発明の原理を説明するための図である。

【０００８】

本発明は、送信者Ａの秘密情報を送信装置Ａから受信者Ｂの受信装置Ｂに伝達する秘匿通信方法において、
受信装置Ｂにおいて、受信者Ｂの公開鍵を第三者に対して復号方法が公知な暗号化方法により暗号化する、鍵暗号化ステップ（ステップ１）と、
受信装置Ｂにおいて、暗号化した公開鍵を送信装置Ａに送る公開鍵送信ステップ（ステップ２）と、
送信装置Ａにおいて、受信装置Ｂから受信した公開鍵を復号化して公開鍵を取り出す公開鍵抽出ステップ（ステップ３）と、
送信装置Ａにおいて、取り出した公開鍵により送信者Ａの秘密情報を暗号化する秘密情報暗号化ステップ（ステップ４）と、

送信装置Ａにおいて、暗号化された秘密情報を受信装置Ｂに送信する秘密情報送信ステップ（ステップ５）と、
受信装置Ｂにおいて、暗号化された秘密情報を受信して、該受信装置Ｂのみが有する秘密鍵を用いて復号化して秘密情報を得る秘密情報復号化ステップ（ステップ６）と、からなる。

【０００９】

また、本発明の鍵暗号化ステップにおいて、
復号方法が公知な暗号化方式として、読み出し方法が公知である電子透かし情報埋め込み技術を用いる。

【００１０】

また、本発明の公開鍵送信ステップにおいて、
電子透かしにより公開鍵を埋め込んだ画像を送信装置Ａに提示し、
送信装置Ａにおいて、
提示された画像をカメラで撮影するステップを含む。

【００１１】

また、本発明の公開鍵送信ステップにおいて、
受信装置Ｂが、電子透かしにより公開鍵を埋め込んだ画像を、電子メールにより送信装置Ａに送る。

【００１２】

また、本発明の公開鍵送信ステップにおいて、
受信装置Ｂが、電子透かしにより公開鍵を埋め込んだ画像を、サーバにアップロードするステップを含み、
公開鍵抽出ステップにおいて、送信装置Ａが、サーバにアップロードされた画像をダウンロードするステップを含む。

【００１３】

また、本発明の公開鍵送信ステップにおいて、
受信装置Ｂが、電子透かしにより公開鍵を埋め込んだ画像を、サーバにアップロードするステップを含み、
公開鍵抽出ステップにおいて送信装置Ａが、サーバにアップロードされた画像をインターネットブラウザにより閲覧するステップを含む。

【００１４】

また、本発明の秘密情報暗号化ステップにおいて、
送信装置Ａが、乱数を電子透かし埋め込み鍵にして、秘密情報を任意の画像に埋め込み、該乱数を公開鍵により暗号化して電子透かし埋め込み済み画像に添付するステップを含む。

【００１５】

また、本発明の秘密情報暗号化ステップにおいて、
送信装置Ａが、乱数を電子透かし埋め込み鍵にして、秘密情報を任意の画像に埋め込み、該乱数を公開鍵により、暗号化したものを読み出し方法が公知の電子透かし方法を用いて、電子透かし埋め込み済み画像に２重に埋め込むステップを含む。

【００１６】

図２は、本発明の原理構成図である。

【００１７】

本発明は、送信者Ａの秘密情報を送信装置Ａ２００から受信者Ｂの受信装置Ｂ１００に伝達する秘匿通信システムであって、
受信装置Ｂ１００は、
受信者Ｂの公開鍵を第三者に対して復号方法が公知な暗号化方法により暗号化する、鍵暗号化手段１１０と、
鍵暗号化手段１１０で暗号化した公開鍵を送信装置Ａに送る公開鍵送信手段１２０と、
送信装置Ａ２００から暗号化された秘密情報を受信して、当該受信装置Ｂ１００のみが有

する秘密鍵を用いて復号化して秘密情報を得る秘密情報復号化手段１３０と、を有し、
送信装置Ａ２００は、
受信装置Ｂ１００から受信した公開鍵を復号化して公開鍵を取り出す公開鍵抽出手段２１０と、
公開鍵抽出手段２１０で取り出した公開鍵により送信者Ａの秘密情報を暗号化する秘密情報暗号化手段２２０と、
秘密情報暗号化手段２２０において、暗号化された秘密情報を受信装置Ｂ１００に送信する秘密情報送信手段２３０と、を有する。

【００１８】

また、本発明の鍵暗号化手段１１０は、復号方法が公知な暗号化方式として、読み出し方法が公知である電子透かし情報埋め込みを用いる。

【００１９】

また、本発明の受信装置Ｂ１００の公開鍵送信手段１２０は、電子透かしにより情報を埋め込んだ画像を送信装置Ａ２００に提示する手段を含み、
送信装置Ａ２００の公開鍵抽出手段２１０は、提示された画像をカメラで撮影する手段を含む。

【００２０】

また、本発明の受信装置Ｂ１００の公開鍵送信手段１２０は、電子透かしにより公開鍵を埋め込んだ画像を、電子メールにより送信装置Ａに送る手段を含む。

【００２１】

また、本発明の受信装置Ｂ１００の公開鍵送信手段１２０、電子透かしにより公開鍵を埋め込んだ画像を、サーバにアップロードする手段を含み、
送信装置Ａ２００の公開鍵抽出手段２１０は、サーバにアップロードされた画像をダウンロードする手段を含む。

【００２２】

また、本発明の受信装置Ｂ１００の公開鍵送信手段１２０は、電子透かしにより公開鍵を埋め込んだ画像を、サーバにアップロードする手段含み、
送信装置Ａ２００の公開鍵抽出手段２１０は、サーバにアップロードされた画像をインターネットブラウザにより閲覧する手段を含む。

【００２３】

また、本発明の送信装置Ａ２００の秘密情報暗号化手段２２０は、乱数を電子透かし埋め込み鍵にして、秘密情報を任意の画像に埋め込み、該乱数を公開鍵により暗号化して電子透かし埋め込み済み画像に添付する手段を含み、
受信装置Ｂ１００の秘密情報復号化手段１３０は、
電子透かし埋め込み済み画像に添付された暗号化された乱数を自分の秘密鍵で復号し、元の乱数を取得し、該乱数を電子透かし読み出し鍵として、該画像から秘密情報を取得する手段を含む。

【００２４】

また、本発明の送信装置Ａ２００の秘密情報暗号化手段２２０は、乱数を電子透かし埋め込み鍵にして、秘密情報を任意の画像に埋め込み、該乱数を公開鍵により、暗号化したものを読み出し方法が公知の電子透かし方法を用いて、電子透かし埋め込み済み画像に２重に埋め込む手段を含み、
受信装置Ｂ１００の秘密情報復号化手段１３０は、
電子透かし埋め込み画像から公知の電子透かし読み出し方法により暗号化された乱数を取得し、該乱数を自分の秘密鍵で復号し、復号された乱数を電子透かし読み出し鍵として、該電子透かし埋め込み画像から秘密情報を取得する手段を含む。

【００２５】

本発明は、秘密情報の送受信を行う端末装置であって、
公開鍵を第三者に対して復号方法が公知な暗号化方式として、読み出し方法が公知である電子透かし情報埋込技術を用いて暗号化し、画像に埋め込む、鍵暗号化手段と、

鍵暗号化手段で暗号化した公開鍵が埋め込まれた画像を、秘密情報を送信する送信装置に送る公開鍵送信手段と、
送信装置から暗号化された秘密情報を受信して、自装置のみが有する秘密鍵を用いて復号化して秘密情報を得る秘密情報復号化手段と、
秘密情報を受信する受信装置から受信した、画像に埋め込まれた公開鍵を抽出して、復号化する公開鍵抽出手段と、
公開鍵抽出手段で取り出した公開鍵により送信者側の秘密情報を暗号化する秘密情報暗号化手段と、
秘密情報暗号化手段において、暗号化された秘密情報を受信装置に送信する秘密情報送信手段と、を有する。

【００２６】
また、本発明の秘密情報暗号化手段は、
乱数を生成し、該乱数を電子透かし埋込鍵として、秘密情報を任意の画像に埋め込み、該乱数を前記公開鍵により暗号化して、電子透かし埋め込み済み画像に添付する手段を含み、
秘密情報復号化手段は、
暗号化された前記乱数を自らの秘密鍵を用いて復号化し、復号化された乱数を受信した画像に埋め込まれている電子透かしの読み出し鍵として、埋め込み済み画像から秘密情報を取得する手段を含む。

【００２７】
また、本発明の秘密情報暗号化手段は、
乱数を生成し、該乱数を電子透かし埋め込み鍵にして、秘密情報を任意の画像に埋め込み、該乱数を前記公開鍵により、暗号化したものを読み出し方法が公知の電子透かし方法を用いて、電子透かし埋め込み済み画像に２重に埋め込む手段を含み、
秘密情報復号化手段は、
公知の電子透かし読み出し方法を用いて、受信した画像に埋め込まれている暗号化乱数を取得し、該暗号化乱数を自らの秘密鍵で復号することにより乱数を取得し、該乱数を電子透かし読み出し鍵として、埋め込み済み画像から秘密情報を取得する手段を含む。

【００２８】
上記のように、本発明は、秘密情報を受信する装置側で公開鍵を暗号化して秘密情報を送信する装置に渡すことにより、秘密情報を送信する側の装置では、公開鍵を取り出し、取り出した公開鍵により秘密情報を暗号化して受信側の装置に渡し、受信側の装置では、自分の秘密鍵を用いて秘密情報を復号化することにより、秘密鍵を持っていない第三者に秘密情報が漏洩しない。

【００２９】
また、秘密情報埋め込みに用いる電子透かしの鍵を、乱数により通信の都度生成し、生成した乱数を公開鍵暗号方式で暗号化して画像に添付する、または、画像に埋め込むことにより、電子透かし鍵を容易に生成して受信者に渡すことが可能となる。

【００３０】
【発明の実施の形態】
以下、図面と共に本発明の実施の形態を説明する。

【００３１】
[第１の実施の形態]
図３は、本発明の第１の実施の形態における秘密情報の送信動作を説明するための図である。

【００３２】
同図において、秘密情報は、秘密情報送信者装置Ａから秘密情報受信者装置Ｂに伝達されるものとする。

【００３３】
秘密情報受信者装置Ｂは、自分の公開鍵を秘密情報送信者装置Ａに伝えるために、読み出

し方法が第三者に公知の暗号化方法で公開鍵を暗号化し（ステップ１０１）、秘密情報送信者装置Ａに送る（ステップ１０２）。秘密情報送信者装置Ａは、公知の復号化方法を用いて秘密情報受信者装置Ｂの公開鍵を得る（ステップ１０３）。秘密情報送信者装置Ａは、秘密情報を秘密情報受信者装置Ｂの公開鍵を用いて暗号化し（ステップ１０４）、秘密情報受信者装置Ｂへ送る（ステップ１０５）。暗号化の方法は、任意の公開鍵暗号方式でよく、例えば、ＲＳＡ暗号を用いる。秘密情報受信者装置Ｂは受け取った暗号化情報を、当該秘密情報受信者装置Ｂだけが持つ秘密鍵で復号化し、秘密情報を得る（ステップ１０６）。

【００３４】

次に、上記の動作を実現するための装置構成について説明する。

【００３５】

図４は、本発明の第１の実施の形態におけるシステム構成を示す。

【００３６】

同図に示すシステムは、秘密情報受信者装置１００と秘密情報送信者装置２００から構成される。

【００３７】

秘密情報受信者装置１００は、秘密情報受信者の公開鍵を第三者に対して復号方法が公知な暗号化方法により暗号化する、鍵暗号化部１１０と、鍵暗号化部１１０で暗号化した公開鍵を送信装置Ａに送る公開鍵送信部１２０と、秘密情報送信装置２００から暗号化された秘密情報を受信して、当該秘密情報受信装置１００のみが有する秘密鍵を用いて復号化して秘密情報を得る秘密情報復号化部１３０と、を有する。

【００３８】

秘密情報送信者装置２００は、秘密情報受信者装置１００から受信した公開鍵を復号化して公開鍵を取り出す公開鍵抽出部２１０と、公開鍵抽出部２１０で取り出した公開鍵により送信者Ａの秘密情報を暗号化する秘密情報暗号化部２２０と、秘密情報暗号化部２２０において、暗号化された秘密情報を秘密情報受信者装置１００に送信する秘密情報送信部２３０と、を有する。

【００３９】

［第２の実施の形態］

本実施の形態では、秘密情報受信者Ｂの公開鍵を電子透かしで画像に埋め込んで秘密情報送信者Ａに送る場合について説明する。

【００４０】

図５は、本発明の第２の実施の形態における秘密情報送信動作を説明するための図である。

【００４１】

秘密情報受信者装置Ｂは、読み出し方法が第三者に公知の電子透かしを用いて、自分の公開鍵を任意の画像に埋め込み（ステップ２０１）、埋め込み済み画像を秘密情報送信者装置Ａに送信する（ステップ２０２）。秘密情報送信者装置Ａは、公知の電子透かし読み出し方法を用いて、秘密情報受信者装置Ｂから受信した埋め込み済み画像から秘密情報受信者装置Ｂの公開鍵を得る（ステップ２０３）。以降の処理は前述の第１の実施の形態と同様であるので、その説明を省略する。

【００４２】

次に、上記の動作を実現するための装置構成について説明する。

【００４３】

図６は、本発明の第２の実施の形態におけるシステム構成を示す。

【００４４】

同図に示すシステムにおいて、図４と同一構成部分については、同一符号を付し、その説明を省略する。

【００４５】

秘密情報受信者装置１００は、秘密情報受信者が有する公開鍵を電子透かしで画像に埋め

込む電子透かし埋込部１１１、電子透かしが埋め込まれた画像を秘密情報送信者装置２００に送信する画像送信部１２１を有する。

【００４６】

秘密情報送信者装置２００は、秘密情報受信者装置１００から送信された電子透かしが埋め込まれた画像から公知の電子透かし読み出し方法により電子透かしを読み出し、秘密情報受信者の公開鍵を抽出する電子透かし読み出し部２１１を有する。

【００４７】

同図において他の構成は図４の構成と同様である。

【００４８】

なお、本実施の形態において、秘密情報受信者装置Ｂから秘密情報送信者装置Ａに対して、公開鍵を電子透かしにより埋め込んだ画像を送信する際に、サーバを介してアップロードし、秘密情報送信者装置Ａがアップロードされた画像をダウンロードすることも可能である。

【００４９】

また、秘密情報受信者装置Ｂから秘密情報送信者装置Ａに対して、公開鍵を電子透かしにより埋め込んだ画像を送信する際に、サーバを介してアップロードし、秘密情報送信者装置Ａがアップロードされた画像をインターネットブラウザにより閲覧することも可能である。

【００５０】

また、サーバを介さずに、秘密情報受信者Ｂが秘密情報受信者装置Ｂ上に電子透かしにより公開鍵を埋め込んだ画像を表示し、秘密情報送信者Ａに提示し、秘密情報送信者装置Ａにより、提示された画像を撮影することにより、当該画像を取得することも可能である。

【００５１】

［第３の実施の形態］

本実施の形態では、秘密情報受信者の公開鍵だけでなく、秘密情報送信者の秘密情報をも電子透かしで画像に埋め込んで秘密情報受信者装置に送信する場合について説明する。

【００５２】

図７は、本発明の第３の実施の形態における秘密情報の送信動作を説明するための図である。

【００５３】

秘密情報受信者装置Ｂは、公開鍵を電子透かしで画像に埋め込んで（ステップ３０１）、秘密情報送信者装置Ａに送り（ステップ３０２）、秘密情報送信者装置Ａは、秘密情報受信者Ｂの公開鍵を得る（ステップ３０３）までは、第２の実施の形態と同様である。秘密情報送信者装置Ａは、任意の乱数を選び、秘密情報受信者Ｂの公開鍵で暗号化する（ステップ３０４）。また、同じ乱数を埋込鍵に用いて、秘密情報を任意の画像に電子透かしで埋め込む（ステップ３０５）。秘密情報送信装置Ａは、埋込済み画像に暗号化された乱数を添付して秘密情報受信者装置Ｂに送る（ステップ３０６）。なお、乱数の添付方法は任意であり、画像ファイルと暗号化乱数ファイルを連続して送るようにしても、または、画像ファイルのヘッダの一部へ暗号化乱数を書き込むようにしてもよい。秘密情報受信者装置Ｂは、電子透かしが埋め込まれた画像に添付された暗号化乱数を自分の秘密鍵で復号し、元の乱数を得る（ステップ３０７）。その乱数を電子透かし読み出し鍵として、埋込済み画像から秘密情報を得る（ステップ３０８）。

【００５４】

次に、上記の動作を実現するための装置構成について説明する。

【００５５】

図８は、本発明の第３の実施の形態におけるシステム構成を示す。

【００５６】

同図に示すシステムにおいて、図６と同一構成部分には同一符号を付し、その説明を省略する。

【００５７】

秘密情報受信装置１００には、図６の構成に加えて、秘密情報送信装置２００から送信される暗号化乱数が付与された画像情報を受信して、暗号化乱数を自分の秘密鍵で復号化する暗号化乱数復号化部１３１を有する。これにより、秘密情報復号化部１３０では、前述の第２の実施の形態で用いていた秘密鍵を用いずに、暗号化乱数復号化部１３１で復号された乱数を電子透かし読み出し鍵として、電子透かしが埋め込まれた埋込済み画像から秘密情報を取得する。

【００５８】

秘密情報送信装置２００は、第２の実施の形態と同様の電子透かし読み出し部２１１と、乱数を生成する乱数生成部２１２、生成された乱数を用いて電子透かし読み出し部２１１で読み出された公開鍵を暗号化する乱数暗号化部２１３、乱数暗号化部２１３で暗号化された乱数を埋込鍵として用いて秘密情報を暗号化する秘密情報暗号化部２２０、秘密情報暗号化部２２０で暗号化された秘密情報に、乱数暗号化部２１３で暗号化された乱数を添付する乱数添付部２２１、乱数添付部２２１で暗号化乱数が添付された暗号化された秘密情報を秘密情報受信装置１００に送信する秘密情報送信部２３０から構成される。

【００５９】

また、本実施の形態では、前述の第２の実施の形態と同様に、秘密情報受信者装置Ｂから秘密情報送信者装置Ａに対して、暗号化された乱数が添付された秘密情報を送信する際に、サーバを介してアップロードし、秘密情報送信者装置Ａがアップロードされた秘密情報をダウンロードすることも可能である。

【００６０】

また、秘密情報受信者装置Ｂから秘密情報送信者装置Ａに対して、暗号化された乱数が添付された秘密情報を送信する際に、サーバを介してアップロードし、秘密情報送信者装置Ａがアップロードされた秘密情報をインターネットブラウザにより閲覧することも可能である。

【００６１】

［第４の実施の形態］

本実施の形態では、秘密情報受信装置Ｂの公開鍵、秘密情報送信装置Ａの秘密情報及び秘密情報送信者が選んだ乱数を全て電子透かしで画像に埋め込んで送る場合について説明する。

【００６２】

図９は、本発明の第４の実施の形態における秘密情報送信動作を説明するための図である。

【００６３】

同図において、ステップ４０１～ステップ４０５までは、前述の第３の実施の形態における図７のステップ３０１～ステップ３０５と同様であるので、その説明は省略する。

【００６４】

秘密情報送信装置Ａでは、秘密情報埋め込み済み画像に対して、読み出し方法が第三者に公知の電子透かしを用いて、暗号化乱数を埋め込み（ステップ４０６）、埋込済み画像を秘密情報受信装置Ｂに送信する（ステップ４０７）。

【００６５】

秘密情報受信装置Ｂは、秘密情報送信装置Ｂから受信した電子透かし埋め込み済み画像から、公知の電子透かし読み出し方法を用いて暗号化乱数を得る（ステップ４０８）。取得した暗号化乱数を自分の秘密鍵で復号し（ステップ４０９）、乱数を得る。その乱数を電子透かし読み出し鍵として、埋め込み済み画像から秘密情報を得る（ステップ４１０）。

【００６６】

次に、上記の動作を実現するための装置構成について説明する。

【００６７】

秘密情報受信装置１００は、前述の第３の実施の形態と同様の電子透かし埋込部１１１、画像送信部１２１と、秘密情報送信装置２００から送信された暗号化乱数が埋め込まれた秘密情報を受信して、公知の電子透かし読み出し方法を用いて暗号化乱数を取得する電子

透かし読み出し部１３２、取得した暗号化乱数を自分の秘密鍵で復号化して乱数を得る暗号化乱数復号化部１３１と、取得した乱数を電子透かし読み出し鍵として用いて、電子透かし埋込画像から秘密情報を得る秘密情報復号化部１３０を有する。

【００６８】

秘密情報送信装置２００は、前述の第３の実施の形態と同様の電子透かし読み出し部２１１、乱数生成部２１２、乱数暗号化部２１３と、秘密情報を電子透かしにより画像に埋め込む秘密情報暗号化部２２０と、秘密情報埋込画像に対して像、乱数暗号化部２１３で暗号化された乱数を公知の電子透かし埋込方法を用いて埋め込む暗号化乱数埋込部２２２、秘密情報埋込画像に暗号化乱数が埋め込まれた画像を秘密情報受信装置１００に送信する秘密情報送信部２３０から構成される。

【００６９】

また、本実施の形態では、前述の第２、第３の実施の形態と同様に、秘密情報受信者装置Ｂから秘密情報送信者装置Ａに対して、暗号化乱数が埋め込まれた秘密情報埋込画像を送信する際に、サーバを介してアップロードし、秘密情報送信者装置Ａがアップロードされた画像をダウンロードすることも可能である。

【００７０】

また、秘密情報受信者装置Ｂから秘密情報送信者装置Ａに対して、暗号化乱数が埋め込まれた秘密情報埋込画像を送信する際に、サーバを介してアップロードし、秘密情報送信者装置Ａがアップロードされた画像をインターネットブラウザにより閲覧することも可能である。

【００７１】

なお、上記の各実施の形態における秘密情報受信者装置１００の公開鍵及び秘密鍵、秘密情報送信者装置２００の秘密情報は、メモリ等の記憶手段に格納されているものとする。

【００７２】

【実施例】

以下、図面と共に本発明の実施例を説明する。

【００７３】

[第１の実施例]

図１１は、本発明の第１の実施例を説明するための図である。

【００７４】

本実施例では、秘密情報受信者装置Ｂ，秘密情報送信者装置Ａとして、カメラ付き携帯電話機を用い、携帯電話機Ａから携帯電話機Ｂのみへ秘密情報（携帯電話番号とメールアドレス等）を伝える状況について説明する。

【００７５】

携帯電話機Ｂは、予め自分の公開鍵を電子透かしにより任意の画像に埋め込み（ステップ５０１）、シールとして携帯電話機や携帯電話機ストラップに貼っておく。シールは、被撮影可能なら任意の品物に貼ってもよい。

【００７６】

携帯電話機Ａは、カメラ付き携帯電話機により携帯電話機Ｂのシールを撮影し（ステップ５０２）、電話機の電子透かし読み取り機能により、携帯電話機Ｂの公開鍵を得る（ステップ５０３）。携帯電話機Ａは、乱数を一つ選び、それを埋め込み鍵として任意の画像に秘密情報を電子透かし方法を用いて埋め込む。乱数は携帯電話機Ｂの公開鍵で暗号化し、暗号化乱数情報を読み出し方法が公知の電子透かしにより秘密情報が埋め込まれた画像へ埋め込む（ステップ５０４）。秘密情報と暗号化乱数が埋め込まれた画像を携帯電話機Ａの表示部に提示し（ステップ５０５）、それを携帯電話機Ｂが撮影する（ステップ５０６）。

【００７７】

携帯電話機Ｂは、撮影画像から公知の電子透かし読み出し方法を用いて暗号化乱数を得る。暗号化乱数と自分の秘密鍵から携帯電話機Ａが透かし埋め込みに用いた乱数を得る。乱数を読み出し鍵として画像から電子透かしを読み出すことにより、携帯電話機Ａで埋め込

まれた秘密情報を得る（ステップ５０７）。

【００７８】

これにより、携帯電話機Ａが秘密情報埋め込み済み画像を提示した際に、携帯電話機Ｂ以外の第三者もその画像を撮影することは可能であるが、秘密鍵を持っている携帯電話機Ｂの利用者以外は秘密情報を読み出せない。

【００７９】

また、携帯電話機Ａの利用者は、秘密情報埋め込みに使用した乱数を暗号化する公開鍵を選ぶことにより、誰に秘密情報を公開するかを選択することができる。

【００８０】

［第２の実施例］

図１２は、本発明の第２の実施例を説明するための図である。

【００８１】

本実施例では、カメラ付き携帯電話機Ａの利用者が、秘密情報と暗号化乱数が埋め込まれた画像をカメラ付き携帯電話機Ｂの利用者に送る際に、インターネットのＷｅｂサーバを経由する（ステップ６０６）点において前述の第１の実施例と異なり、他は第１の実施例と同様である。

【００８２】

［第３の実施例］

図１３は、本発明の第３の実施例を説明するための図である。

【００８３】

本実施例では、カメラ付き携帯電話機Ａの利用者が秘密情報と暗号化乱数が埋め込まれた画像をカメラ付き携帯電話機Ｂの利用者に送る際に、赤外線通信による（ステップ７０６）点において前述の第１の実施例と異なり、他は第１の実施例と同様である。

【００８４】

なお、上記の実施の形態及び実施例では、秘密情報送信者装置と秘密情報受信者装置に分けて説明したが、１つの装置（端末装置）で送受信双方の機能を備えるものとする。

【００８５】

また、上記の実施の形態及び実施例における秘密情報送信者装置の動作を、送信時の動作として、また、秘密情報受信者装置の動作を受信時の動作としてプログラムを構築し、携帯電話機等の制御手段を有する装置にインストールする、または、ネットワークを介して流通させることも可能である。

【００８６】

なお、本発明は、上記の実施の形態及び実施例に限定されることなく、特許請求の範囲内において種々変更・応用が可能である。

【００８７】

【発明の効果】

上述のように本発明によれば、秘密情報送信者Ａが提示した秘密情報が埋め込まれた画像は、任意の第三者が取得することはできるが、透かし埋め込み鍵を復号する秘密鍵を持っている秘密情報受信者Ｂのみがその秘密情報を知ることができる。秘密情報送信者Ａは、透かし埋め込みに使用した乱数を暗号化する公開鍵を選ぶことにより、誰に秘密情報を公開するかを選択することができる。

【図面の簡単な説明】

【図１】本発明の原理を説明するための図である。

【図２】本発明の原理構成図である。

【図３】本発明の第１の実施の形態における秘密情報の送信動作を説明するための図である。

【図４】本発明の第１の実施の形態におけるシステム構成図である。

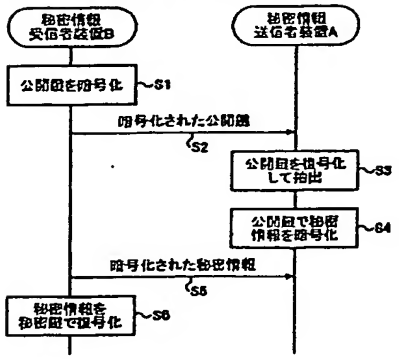
【図５】本発明の第２の実施の形態における秘密情報の送信動作を説明するための図である。

【図６】本発明の第２の実施の形態におけるシステム構成図である。

【図７】本発明の第３の実施の形態における秘密情報の送信動作を説明するための図である。
【図８】本発明の第３の実施の形態におけるシステム構成図である。
【図９】本発明の第４の実施の形態における秘密情報の送信動作を説明するための図である。
【図１０】本発明の第４の実施の形態におけるシステム構成図である。
【図１１】本発明の第１の実施例を説明するための図である。
【図１２】本発明の第２の実施例を説明するための図である。
【図１３】本発明の第３の実施例を説明するための図である。
【符号の説明】
１００　秘密情報受信者装置
１１０　鍵暗号化手段、鍵暗号化部
１１１　電子透かし埋込部
１２０　公開鍵送信手段、公開鍵送信部
１２１　画像送信部
１３０　秘密情報復号化手段、秘密情報復号化部
１３１　暗号化乱数復号化部
１３２　電子透かし読み出し部
２００　秘密情報送信者装置
２１０　公開鍵抽出手段、公開鍵抽出部
２１１　電子透かし読み出し部
２１２　乱数生成部
２１３　乱数暗号化部
２２０　秘密情報暗号化手段、秘密情報暗号化部
２２１　乱数添付部
２２２　暗号化乱数埋込部
２３０　秘密情報送信手段、秘密情報送信部

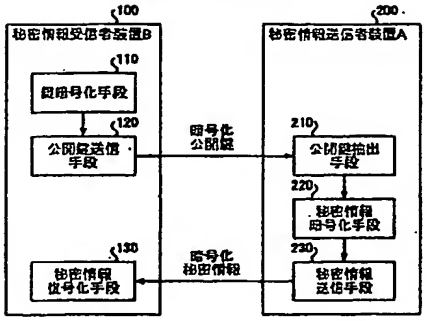
【図１】

本発明の原理を説明するための図



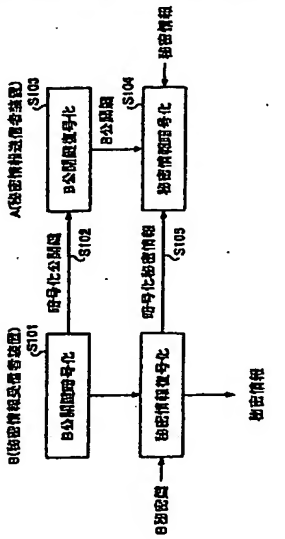
【図２】

本発明の原理構成図



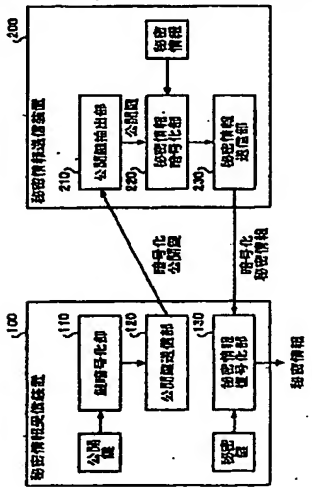
【図３】

本発明の第１の実施の形態における
秘密情報の送信動作を説明するための図



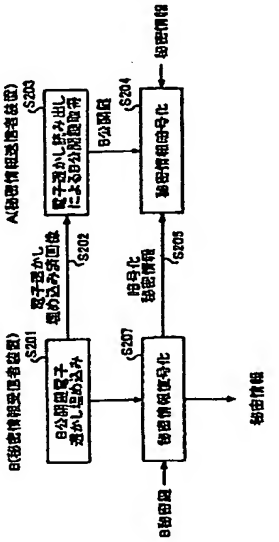
【図４】

本発明の第１の実施の形態におけるシステム構成図



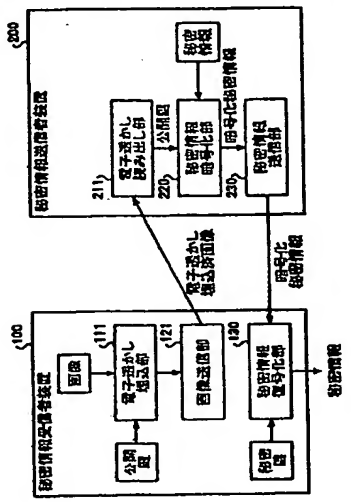
【図５】

本発明の第2の実施の形態における
秘密情報の送信動作を説明するための図



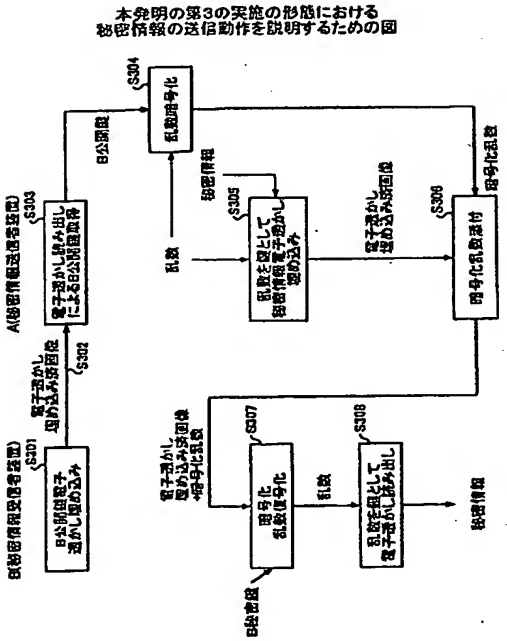
【図６】

本発明の第2の実施の形態におけるシステム構成図



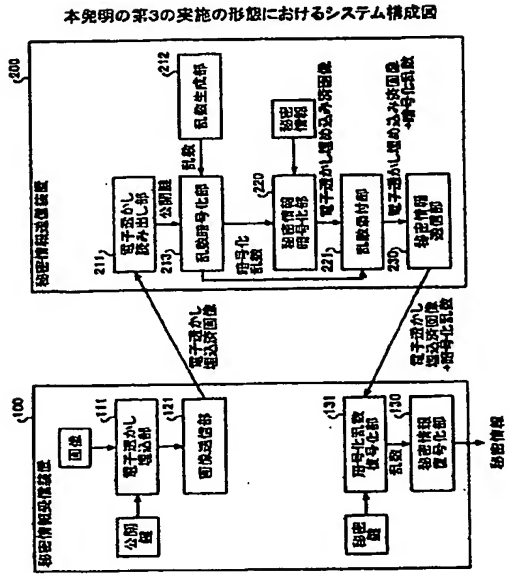
【図７】

本発明の第3の実施の形態における
秘密情報の送信動作を説明するための図



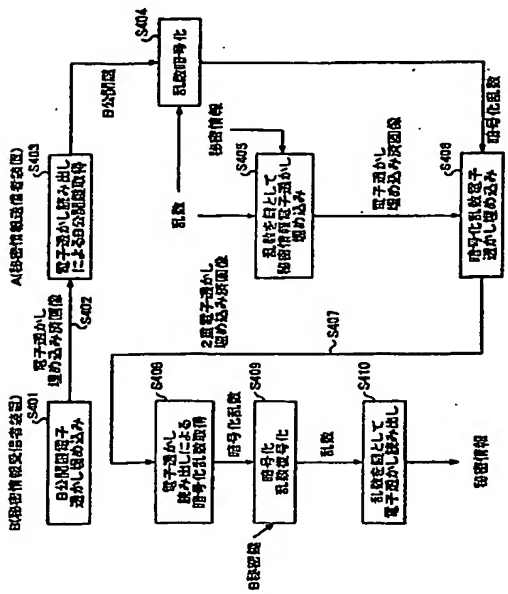
【図８】

本発明の第3の実施の形態におけるシステム構成図



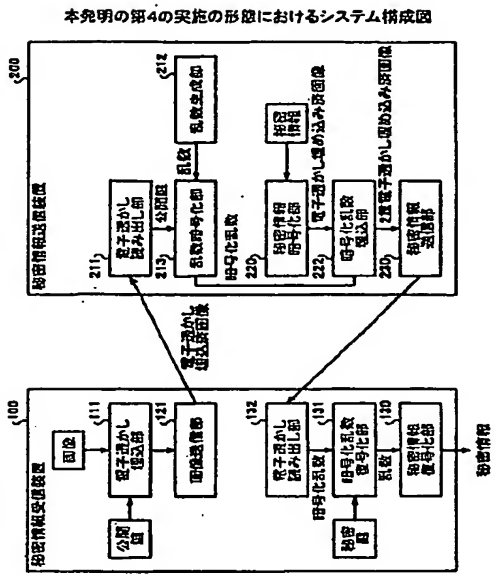
【図９】

本発明の第4の実施の形態における
秘密情報の送信動作を説明するための図



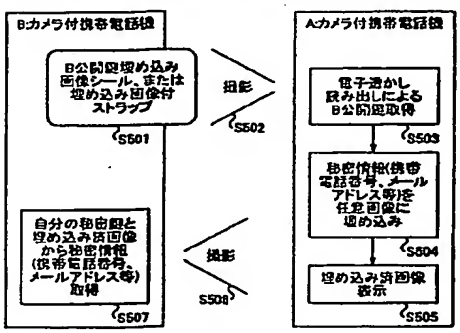
【図１０】

本発明の第4の実施の形態におけるシステム構成図



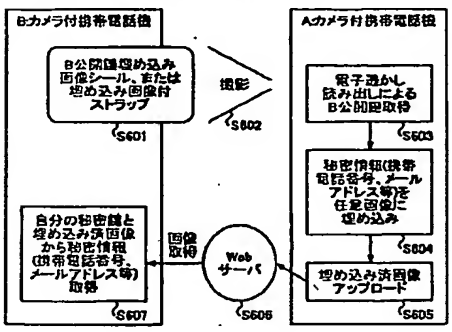
【図１１】

本発明の第1実施例を説明するための図



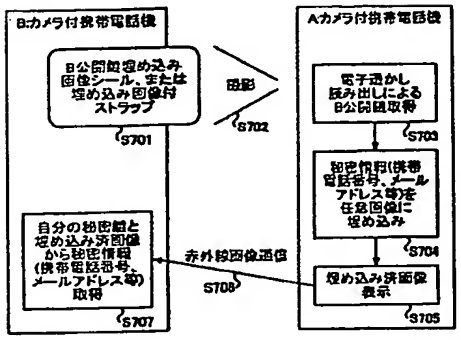
【図１２】

本発明の第2実施例を説明するための図



【図１３】

本発明の第3実施例を説明するための図



フロントページの続き

Fターム(参考) 5B057 AA20 CA12 CB12 CB19 CE08 CF01 CG09 CH01 CH14
5C076 AA14 BA06 BA09
5J104 EA17 EA19